

**IN THE UNITED STATES PATENT & TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

IN RE APPLICATION OF:
RYAN CHARLES CATHERMAN

SERIAL NO.: **10/750,594**

FILED: **12/31/2003**

TITLE: **METHOD FOR
SECURELY CREATING AND
ENDORSEMENT CERTIFICATE IN
AN INSECURE ENVIRONMENT**

§ ATTORNEY DOCKET
§ NO.: **RPS920030206US1**
§
§ EXAMINER: **NIRAV PATEL**
§
§ GROUP ART UNIT: **2135**
§
§ CONFIRMATION NO. **8589**
§
§
§

APPEAL BRIEF UNDER 37 C.F.R. 41.37

Mail Stop Appeal Briefs - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This Appeal Brief is submitted in support of the Appeal of the Examiner's final rejection of Claims 1, 5-8 and 10 in the above-identified application. A Notice of Appeal was filed on February 17, 2009. Please charge a one month extension of time to **Dillon & Yudell LLP Account No. 50-3083**. Please charge any additional fees required to **IBM Corporation Deposit Account No. 50-0563**.

REAL PARTY IN INTEREST

The real party in interest in the present Appeal is International Business Machines Corporation, the Assignee of the present application as evidenced by the assignment recorded at Frame 0259 of Reel 014808.

RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences known to Appellants, the Appellants' legal representative, or assignee, which directly affect or would be directly affected by or have a bearing on the Board's decision in the pending Appeal.

STATUS OF CLAIMS

Claims 1 - 25 were originally presented. Claims 2-4, 9, and 11-25 were cancelled during prosecution. Claims 1, 5-8 and 10, which comprise all pending claims, stand finally rejected by the Examiner as noted in the Final Office Action dated November 14, 2008. The rejection of each of Claims 1, 5-8 and 10 is appealed.

STATUS OF AMENDMENTS

Appellants' Amendment D, dated October 9, 2008, was entered by the Examiner. No amendments to the claims have been proposed or entered subsequent to the final rejection that leads to this appeal.

SUMMARY OF THE CLAIMED SUBJECT MATTER

Appellants' independent Claim 1 recites a method for securely creating an endorsement certificate for a device in an insecure environment. According to the method, an endorsement key pair, including a private key and a public key, is generated for a valid device (Page 11, ¶[0035], FIG. 3, block 340). The private key is not public readable (Page 12, ¶[0042]). A non-public, secure value is created and provided to both a plurality of valid devices and a credential server (Pages 12-13, ¶¶[0040]-[0044]). The value is a first value that is provided to a first set of the plurality of valid devices and a second set of the plurality of valid devices are provided a second value (Page 12, ¶[0039]), based on a pre-defined method for determining when to change the first value to the second value from among: a passage of a pre-set amount of device

manufacturing time (Page 12, ¶[0039]) and a preset number of manufactured devices from among the plurality of valid devices (Page 12, ¶[0039]), wherein the non-public, secure value is a secret number (Page 12, ¶[0039]). A first copy of the secret number is transmitted, via a secure communication medium, to the credential server (Page 10, ¶[0030], Pages 12-13 ¶¶[0041]-[0042], FIG. 4, block 405). A second copy of the secret number is hashed with a public key from the endorsement key pair (Page 6, ¶[0016], Page 6, ¶[0019], FIG. 4, block 411). A first hash result from the hashing step is combined with the public key to create an endorsement key (EK) (Page 13, ¶¶[0042]-[0044], FIG. 4, blocks 411-413). The EK is transmitted to the credential server to initiate a credential process (Page 13, ¶[0045], FIG. 4, block 415). The endorsement key of the valid device is verified by utilizing the non-public, secure value that a valid endorsement key of the endorsement key pair that was generated during manufacture of the valid device (Page 14, ¶[0047], FIG. 4, blocks 417), wherein a function of a first copy of the non-public, secure value within the credential server matches a similar function of a second copy of the non-public, secure value associated with the endorsement key received at the credential server (Page 14, ¶[0047]). The verifying process also further comprises: receiving the EK from the device at the credential server (Page 14, ¶[0047]), calculating an expected hash value by hashing the public key within the received EK with the first copy of the secret number received during the transmitting step (Page 14, ¶[0047], FIG. 4, block 416), comparing the first hashed value from within the EK with the expected hash value (Page 14, ¶[0047], FIG. 4, block 417), and confirming the EK is from a valid device when the comparing step results in a match (Page 14, ¶[0047], FIG. 4, block 417-418). In response to confirming the EK is from a valid device, an endorsement certificate is inserted into the device to indicate that the device is an approved device by an original equipment manufacturer (OEM) of the device (Page 14, ¶¶[0047]-[0048], FIG. 4, block 421).

In addition to the features of independent Claim 1, Claim 5 recites that the verifying step of the method further comprises: initially storing the credential in a database of the credential server (Page 10, ¶[0030], Pages 12-13 ¶¶[0041]-[0042], Page 14 ¶[0049]); monitoring for a request from a customer to provide the certificate to the device (Page 14, ¶[0050], FIG. 5, block 504); and following a receipt of the customer request, transmitting the certificate to the device to be inserted within the device (Page 14, ¶[0050], FIG. 5, block 505).

Appellants' Claim 6 further recites that the endorsement certificate is once-writeable public-readable and is utilized for signing the public key during communication from and to the device (Page 11, ¶[0036], Page 14, ¶[0048]).

Claim 7 also recites the value is injected into the device, and the value is a single-use parameter, immediately destroying the value within the device following a creation of the EK (Page 6, ¶[0017], Page 5, ¶[0019], Page 13, ¶[0042], Page 13, ¶[0044]).

Claim 8 recites that the credential server is remotely located from a vendor manufacturing the device and the value is communicated from the device to the credential server via a secure communication medium (Page 10, ¶[0030]-[0031], Page 10, ¶[0033]).

Finally, Claim 10 recites that the device is a trusted platform module (TPM) (Page 10, ¶[0032]).

GROUND OF REJECTION TO BE REVIEWED ON APPEAL

The grounds of rejection to be reviewed on appeal are:

(a) the final rejection of Claims 1, 5, 6, 8, and 10 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,892,302 to Wheeler et al. (hereafter *Wheeler*) in view of U.S. Patent No. 6,513,117 to Tarpenning et al. (hereafter *Tarpenning*) in view of US Pub. No. 2002/0199110 in view of Kean (hereinafter *Kean*) in view of U.S. Pub No. 2002/0199110 to Multerer et al. (hereafter *Multerer*) in view of U.S. Patent No. 7,142,674 to Brickell et al. (hereafter *Brickell*); and

(b) the final rejection of Claim 7 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,892,302 to Wheeler et al. (hereafter *Wheeler*) in view of U.S. Patent No. 6,513,117 to Tarpenning et al. (hereafter *Tarpenning*) in view of US Pub. No. 2002/0199110 in view of Kean (hereinafter *Kean*) in view of U.S. Pub No. 2002/0199110 to Multerer et al. (hereafter *Multerer*) in view of U.S. Patent No. 7,142,674 to Brickell et al. (hereafter *Brickell*) in view of US Pub. No. 2006/0072747 to Wood et al (hereinafter *Wood*).

ARGUMENT

I. Examiner's rejection of Claims 1, 5, 6, 8, and 10 under 35 U.S.C. § 103(a) is not well founded and should be reversed.

On page 4 of the Final Office Action, Claims 1, 5, 6, 8, and 10 are rejected under 35 U.S.C. § 103(a) as being unpatentable over *Wheeler* in view of *Tarpenning* in view of *Kean* in view of *Multerer* in view of *Brickell*. The rejection is not well founded and should be reversed.

A. General requirements for a claim rejection under 35 U.S.C. § 103

According to 35 U.S.C. § 103(a):

A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

In order to make the obviousness determination, the U.S. Supreme Court held in *Graham v. John Deere Co.*, 383 U.S. 1 (1966) (hereinafter *John Deere*) that three factors must be considered:

- (1) the scope and content of the pertinent prior art;
- (2) differences between the pertinent prior art and the invention at issue; and
- (3) the ordinary level of skill in the pertinent art.

B. Rejection of Claim 1 should be reversed

The final rejection of exemplary Claim 1 under 35 U.S.C. § 103 should be reversed because the combination of *Wheeler*, *Tarpenning*, *Kean*, *Multerer*, and *Brickell* does not disclose or render obvious each feature of the claim, and in particular, does not disclose or render obvious the following features of exemplary Claim 1:

- (a) combining a first hash result from said hashing step with the public key to create an endorsement key (EK);

- (b) calculating an expected hash value by hashing the public key within the received EK with the first copy of said secret number received during said transmitting step;
- (c) comparing the first hashed value from within the EK with the expected hash value;

1. The combination of cited references does not disclose or render obvious the “combining” feature, as recited in Claim 1.

The final rejection of Claim 1 should be reversed because the combination of *Wheeler, Tarpenning, Kean, Multerer, and Brickell* does not disclose or render obvious “combining a first hash result from said hashing step with the public key to create an endorsement key (EK)”, as recited in Appellants’ Claim 1.

At page 5 of the present Office Action, the Examiner cites col. 4 lines 48-50 of *Brickell* as teaching the “combining feature”. However, a careful reading of *Brickell* and specifically the cited sections of *Brickell* fail to teach or suggest Appellants’ combining feature. Specifically, col. 4 lines 48-50 of *Brickell* discloses: “[a]t block 106, the processor sends a first command, the first hash value and the processor’s public key to the peripheral. Furthermore, col. 4 lines 29-47 of *Brickell* recites “At block 104, the processor generates a first hash value by applying a hash algorithm using the short nonce, the long nonce, and the public key generated in block 100 as input parameters”. *Brickell* further continues to disclose the short nonce and the long nonce as “a sequence of bits randomly generated by a random number generator” (see at least Col. 4 lines 20-47). Accordingly, the method disclosed by *Brickell* comprises the processor sending three separate data entities to the peripheral: a randomly generated number pair (the short and long nonce pair), a command, and a processor’s public key. Additionally, col. 4, lines 50-51 discloses “[t]his data may be sent to the peripheral in one or more separate transfers.”

In contrast, Appellants’ Claim 1 recites: “combining a first hash result from said hashing step with the public key to create an endorsement key (EK)”. In direct contrast to *Brickell*, Claim 1 provides that the EK is created at a valid device and transmitted to the credential server “to initiate a credential process”, instead of creating three separate data entities at a processor and sending the three separate data entities to a peripheral, as disclosed by *Brickell*. The EK, as utilized within Appellants’ claimed invention, is comprised of a private key (not public readable)

and a public key. The private key portion of the EK further comprises a secret number which is hashed with a public key. The secret number, as recited within the claims, is “provided to both a plurality of valid devices and a credential server”. The valid device is therefore able to create and wholly transmit the EK, in a singular transmission, to a credential server to initiate the credential process. Neither *Brickell*, nor a combination of the cited references, discloses or renders obvious “combining a first hash result from said hashing step with the public key to create an endorsement key (EK)”, as recited in Appellants’ Claim 1. The rejection of Claim 1 under 35 U.S.C. § 103 should therefore be reversed.

2. Combination of cited references does not disclose or render obvious the “calculating” feature, as recited in Claim 1.

The final rejection of Claim 1 should also be reversed because the combination of *Wheeler, Tarpenning, Kean, Multerer*, and *Brickell* does not disclose “calculating an expected hash value by hashing the public key within the received EK with the first copy of said secret number received during said transmitting step,” as recited in Appellant’s Claim 1.

At page 5 of the present Office Action, the Examiner cites to Fig. 3 and col. 6 lines 6-16 of *Brickell* as teaching Appellants’ calculating feature. However, the cited sections of *Brickell* merely disclose comparing a hash of a short nonce, long nonce, and a processor’s public key computed by the peripheral with the first hash value received from the processor. Specifically, col. 6 lines 6-16 of *Brickell* recites:

... At block 122, the peripheral checks that the hash of the short nonce, long nonce, and the processor's public key matches the first hash value sent to the peripheral by the processor (at block 106). The same hash algorithms must be used. For example, if the SHA-1 hash algorithm was used at block 104, then the SHA-1 algorithm must be used at block 122.

If the first hash value received from the processor equals the hash value computed by the peripheral, then the peripheral is assured that the peripheral actually received the processor's legitimate public key. When the hash values match, the peripheral activates the trust indicator to indicate a second mode or state (e.g., an "OK" state) at block 124.

From reading the above cited sections, it is clear that *Brickell* discloses the peripheral checking a hash value received from the processor with the hash value computed by the

peripheral. In this manner the peripheral is checking that it has received a valid key from the processor, for example, col 6, lines 12-15 of *Brickell* recites: “If the first hash value received from the processor equals the hash value computed by the peripheral, then the peripheral is assured that the peripheral actually received the processor’s legitimate public key.” It is obvious from the cited sections that *Brickell* is solely concerned with a peripheral checking a hash value received from a processor.

In direct contrast, Appellants’ Claim 1 recites “calculating an expected hash value by hashing the public key within the received EK with the first copy of said secret number received during said transmitting step”. The transmitting step clearly recites: “transmitting said EK to said credential server to initiate a credential process”. Accordingly, the calculating of an expected hash value, as claimed, occurs at the credential server, instead of at a peripheral, as disclosed by *Brickell*.

Appellants submit that to support a finding of “obviousness, the Examiner must show that each and every limitation of the claim is described or suggested by the prior art or would have been obvious based on the knowledge of those of ordinary skill in the art.” *Ex parte Newcomb*, Bd. of Pat. App. and Int. (March 31, 2008), citing *In re Fine*, 837 F.2d 1071, 1074 (Fed. Cir. 1988); see also, *CFMT, Inc. v. Yieldup Int’l Corp.*, 349 F.3d 1333, 1342 (Fed. Cir. 2003) (“[O]bviousness requires a suggestion of all the elements in a claim.”).

The Manual of Patent Examination Procedure states that “the examiner should be fully aware of what the claims do not call for, as well as what they do require.” *MPEP §904.01*. (first emphasis in original, second emphasis added). In fact, it is well established that “[a]ll words in a claim must be considered in judging the patentability of [a] claim against the prior art.” *In re Wilson*, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970), quoted in *MPEP § 2143.03*. Moreover, “rejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.” *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006) (quoted with approval in *KSR Int’l Co. v. Teleflex Inc.*, 127 S. Ct. 1727, 1741 (2007)).

Neither *Brickell*, nor a combination of the cited references, discloses or renders obvious “calculating an expected hash value by hashing the public key within the received EK with the first copy of said secret number received during said transmitting step”, as recited in Appellants’ Claim 1. The rejection of Claim 1 under 35 U.S.C. § 103 should therefore be reversed.

C. Rejection of Claim 5 should be reversed

The final rejection of Claim 5, under 35 U.S.C. § 103(a) should be reversed for at least the reasons set forth above with reference to underlying Claim 1, from which Claim 5 depends.

D. Rejection of Claim 6 should be reversed

The final rejection of Claim 6, under 35 U.S.C. § 103(a) should be reversed for at least the reasons set forth above with reference to underlying Claim 1, from which Claim 6 depends.

E. Rejection of Claim 8 should be reversed

The final rejection of Claim 8, under 35 U.S.C. § 103(a) should be reversed for at least the reasons set forth above with reference to underlying Claim 1, from which Claim 8 depends.

II. The Examiner’s rejection of Claim 7 under 35 U.S.C. § 103(a) is not well founded and should be reversed

On page 6 of the Final Office Action, Claim 7 is rejected under 35 U.S.C. § 103(a) as being unpatentable over *Wheeler* in view of *Tarpenning* in view of *Kean* in view of *Multerer* in view of *Brickell* in view of *Wood*. The rejection is not well founded and should be reversed.

A. The rejection of Claim 7 should be reversed

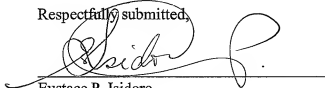
Claim 7 depends from Claim 1, which Appellants have shown to be allowable over the references proffered in the Final Office Action. None of the present references teach or suggest, either individually or in combination, any of the above discussed features of Appellants’ independent Claim 1. Therefore, the final rejection of Claim 7, under 35 U.S.C. § 103(a) should be reversed for at least the reasons set forth above with reference to underlying Claim 1, from which Claim 7 depends.

CONCLUSION

The foregoing remarks demonstrate that the various combinations of cited references do not disclose or render obvious each feature of Appellants' Claims 1, 5-8, and 11, as required to support the final rejections under 35 U.S.C. § 103. Appellants therefore respectfully request the Board to reverse the rejection of each pending claim and issue a notice of allowance for all pending claims.

Applicants further respectfully request the Examiner contact the undersigned attorney of record at 512.343.6116 if such would further or expedite the prosecution of the present Application.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'E. Isidore', is written over a horizontal line.

Eustace P. Isidore

Reg. No. 56,104

DILLON & YUDELL LLP

8911 N. Capital of Texas Highway
Suite 2110

Austin, Texas 78759

(512) 343-6116

ATTORNEY FOR APPELLANTS

CLAIMS APPENDIX

1. A method for securely creating an endorsement certificate for a device in an insecure environment, said method comprising:

generating for a valid device an endorsement key pair that includes a private key and a public key, wherein said private key is not public readable;

creating a non-public, secure value that is provided to both a plurality of valid devices and a credential server, wherein the value is a first value that is provided to a first set of said plurality of valid devices and a second set of said plurality of valid devices are provided a second value, based on a pre-defined method for determining when to change said first value to said second value from among: a passage of a pre-set amount of device manufacturing time and a preset number of manufactured devices from among the plurality of valid devices, wherein said non-public, secure value is a secret number;

transmitting a first copy of said secret number via a secure communication medium to said credential server;

hashing a second copy of said secret number with a public key from said endorsement key pair;

combining a first hash result from said hashing step with the public key to create an endorsement key (EK);

transmitting said EK to said credential server to initiate a credential process;

verifying by utilizing said non-public, secure value that an endorsement key of said valid device is a valid endorsement key of said endorsement key pair that was generated during manufacture of said valid device, wherein a function of a first copy of said non-public, secure value within said credential server matches a similar function of a second copy of said non-public, secure value associated with the endorsement key received at the credential server, said verifying step further comprising:

receiving said EK from said device at the credential server,

calculating an expected hash value by hashing the public key within the received EK with the first copy of said secret number received during said transmitting step,

comparing the first hashed value from within the EK with the expected hash value, and

confirming said EK is from a valid device when said comparing step results in a match; and

in response to confirming said EK is from a valid device, inserting an endorsement certificate into said device to indicate that said device is an approved device by an original equipment manufacturer (OEM) of the device.

2 - 4. (canceled)

5. The method of Claim 1, wherein following said verifying step said method further comprises:

initially storing the credential in a database of said credential server;

monitoring for a request from a customer to provide said certificate to said device; and

following a receipt of said customer request, transmitting said certificate to said device to be inserted within the device.

6. The method of Claim 1, wherein said endorsement certificate is once-writeable public-readable and is utilized for signing said public key during communication from and to said device.

7. The method of Claim 1, wherein said value is injected into said device, and said value is a single-use parameter, said method further comprising immediately destroying said value within said device following a creation of said EK.

8. The method of Claim 1, wherein said credential server is remotely located from a vendor manufacturing said device and said method comprises communicating said value from said device to said credential server via a secure communication medium.

9. (canceled)

10. The method of Claim 1, wherein said device is a trusted platform module (TPM).

11-25. (canceled)

EVIDENCE APPENDIX

(NONE)

APPENDIX C
RELATED PROCEEDINGS AND INTERFERENCES

(NONE)